A Note On Verifying Solutions and the Concrete Hardness of the LWE

Jacob Alperin-Sheriff Daniel Apon

July 2, 2019

Abstract

1 Introduction

In Regev's celebrated reduction of worst-case lattice problems to LWE [Reg09], the (lack of) tightness stemming from Lemma 3.6 (Verifying solutions of LWE), has recently been claimed by Sarkar and Singha in [SS19] to be the cause of most of the loss of tightness for dimensions from 2 to 187849, where it is computed to be so overwhelmingly large that Regev's reduction is completely vacuous for all parameters in that range.

1.1 Previous Work on Tightness

A previous work by Chatterjee et al [CKMS16] showed that, for modulus $q = n^2$, and noise parameter $\alpha = 1/(\sqrt{n}\log^2(n))$ (as set by Regev in his proposed decision LWE-based public key cryptosystem), Regev's reduction has, for an algorithm given $m = n^c$ samples, that solves decision LWE for a fraction $1/n^{d_1}$ of all $\mathbf{s} \in \mathbb{Z}_q^n$ with advantage at least $1/n^{d_2}$, has an enormous tightness gap in solving SIVP, namely

$$O(n^{11+c+d_1+2d_2})$$

While this gives a tightness gap far larger than the cost of the best-known algorithms in solving SIVP for commonly used parameters(**Jacob:** TODO: cite) ,

1.2 Towards Relevance for NIST Candidate Algorithms

In terms of 2nd round submissions to NIST, Frodo appears to be the only scheme to which this result is potentially relevant.

Round5, the other 2nd round NIST submission using unstructured lattices, is both based on the *Learning with Rounding* problem and makes use of a sparse secret distribution, which appears to make Regev's reduction totally irrelevant.[1]

To attempt to determine what parameters Frodo needs to be scaled up to in order to claim a non-vacuous reduction even in the random oracle model, the reduction ought to be analyzed with respect to a proper noise parameter α is the primary

(**Jacob:** TODO: describe why the LWE in the public key is the meaningful one for the reduction, e.g. if there exists an LWE adversary which breaks on the higher-noise samples in Enc, we can transform it into an adversary that breaks on the public key alone by creating the necessary additional samples from the public key)

In addition, in an actual run of the protocol, the "bad cases" of

For the public key,

2 Classical Reduction for Learning With Errors

Here we calculate the concrete tightness of the *classical* reduction of GapSVP to LWE obtained by combining the classical portion of Regev's reduction, Peikert's

[1] this does not mean Round5 is insecure, only that it is much much farther from being covered by a reduction than Frodo is

reduction in [Pei08], and Brakerski et al.'s reduction in [BLP^{+}13]

(**Jacob:** TODO: worth noting how much better the reduction is under their plausible tighter parameters, see if it's worth trying to find a proof of)

Lemma 2.1 (Lemma 3.6, [GG00])**.** *Let S_0 be a unit n-dimensional ball at the origin, S_ϵ be a unit n-dimensional ball at distance ϵ from the origin. Then*

$$\frac{vol(S_0 \cap S_\epsilon)}{vol(S_0)} > \epsilon(1-\epsilon^2)^{(n-1)/2}\frac{\sqrt{n}}{3}$$

Corollary 2.2. *For constants $c, d > 0$ and any $\mathbf{z} \in \mathbb{R}^n$ with $\|z\| \leq d$ and $d' = d \cdot \sqrt{n/(c \log n)}$, we have*

$$\Delta(U(d' \cdot \mathcal{B}_n), U(\mathbf{z} + d' \cdot \mathcal{B}_n)) \leq 1 - n^{-c}(c \log n/4)$$

(**Jacob:** Check params)

(**Jacob:** First write in terms of each call to Regev's reduction)

- Let C_2 be the cost of sampling a point $\mathbf{w}$ uniformly at random to sufficient precision from the ball $d' \cdot \mathcal{B}^n$.
- Let C_3 be the cost of reducing $\mathbf{w}$ modulo $\mathbf{B}$, so $C_3 = O(n^2)$
- NO Instance:
  - Each call to Regev's reduction with $(\mathbf{B}, \mathbf{x})$ will have cost C_1, and succeeds when $(\mathbf{B}, \mathbf{d})$ is a NO instance (i.e. $\lambda_1(\mathcal{L}) > \gamma d$) with probability p_1 (p_1 will have to be exponentially close to 1, but how close matters in optimizing parameters). Note that C_1 needs to incorporate the cost of sampling from $D_{\Lambda^*,r}$ with sufficient precision ((**Jacob:** does using the GPV08 sampling algorithm instead of that bootstrapping stuff as Peikert's paper assumes is happening, reduce the concrete cost of Regev's algorithm at all?))
  - N total calls are made to Regev's reduction.
  - Thus, in a NO instance, we do $O((C_1 + C_2 + C_3)N)$ work and accept with probability p_1^N. C_1 should dwarf C_2 and C_3.

Acknowledgments

This work was performed under financial assistance award 70NANB15H328 from the U.S. Department of Commerce, National Institute of Standards and Technology.

References

[BLP^{+}13] Zvika Brakerski, Adeline Langlois, Chris Peikert, Oded Regev, and Damien Stehlé. Classical hardness of learning with errors. *CoRR*, abs/1306.0281, 2013.

[CKMS16] Sanjit Chatterjee, Neal Koblitz, Alfred Menezes, and Palash Sarkar. Another look at tightness II: practical issues in cryptography. In *Paradigms in Cryptology - Mycrypt 2016. Malicious and Exploratory Cryptology - Second International Conference, Mycrypt 2016, Kuala Lumpur, Malaysia, December 1-2, 2016, Revised Selected Papers*, pages 21–55, 2016.

[GG00] Oded Goldreich and Shafi Goldwasser. On the limits of nonapproximability of lattice problems. *J. Comput. Syst. Sci.*, 60(3):540–563, 2000. Preliminary version in STOC 1998.

[Pei08] Chris Peikert. Public-key cryptosystems from the worst-case shortest vector problem. *Electronic Colloquium on Computational Complexity (ECCC)*, 15(100), 2008.

[Reg09] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. *J. ACM*, 56(6):1–40, 2009. Preliminary version in STOC 2005.

[SS19] Palash Sarkar and Subhadip Singha. Verifying solutions to lwe with implications for concrete security. Cryptology ePrint Archive, Report 2019/728, 2019. `https://eprint.iacr.org/2019/728`.